**CLARKSON LAW FIRM, P.C.**
Ryan J. Clarkson (SBN 257074)
*rclarkson@clarksonlawfirm.com*
Yana Hart (SBN 306499)
*yhart@clarksonlawfirm.com*
Mark Richards (SBN 321252)
*mrichards@clarksonlawfirm.com*
Tiara Avaness (SBN 343928)
*tavaness@clarksonlawfirm.com*
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

*Counsel for Plaintiffs and the Proposed Class*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

**UNITED STATES DISTRICT COURT**

**CENTRAL DISTRICT OF CALIFORNIA**

MATTHEW ROUILLARD and KRISTY MUNDEN, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

SAG-AFTRA HEALTH PLAN,

Defendant.

Case No. 2:24-cv-10503

**CLASS ACTION COMPLAINT**

1. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW BUSINESS & PROFESSIONS CODE § 17200, *et seq*.;
2. VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CALIFORNIA CIVIL CODE § 56, *et seq*;
3. DECEIT BY CONCEALMENT, CALIFORNIA CIVIL CODE §§ 1709, 1710;
4. NEGLIGENCE
5. BREACH OF EXPRESS WARRANTY
6. INVASION OF PRIVACY
7. UNJUST ENRICHMENT

**DEMAND FOR JURY TRIAL**

Plaintiffs Matthew Rouillard and Kristy Munden, individually and on behalf of all others similarly situated, ("**Plaintiffs**") brings this Action against SAG-AFTRA

Health Plan ("**SAG Health**" or "**Defendant**"). Plaintiffs' allegations are based upon personal knowledge as to themselves and their own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiffs' attorneys. Plaintiffs believe that substantial additional evidentiary support will exist for the allegations set forth herein, after a reasonable opportunity for discovery.

## INTRODUCTION

1. SAG Health provides a comprehensive health care benefits program for eligible participants and their dependents in the entertainment industry. Entertainment workers can earn eligibility through employment with producers who have signed a collective bargaining agreement with the entertainment industry's largest union: the Screen Actors Guild-American Federation of Television and Radio Artists ("**SAG-AFTRA**"). Tens of thousands of SAG-AFTRA members have availed themselves of SAG Health's offerings, which includes a wide range of medical services.

2. To obtain any of these services, members are required to entrust SAG Health with their highly sensitive and personally identifiable information ("**PII**") and personal health information ("**PHI**"), which SAG Health uses to engage in its usual business activities. SAG Health understands that it has an enormous responsibility to protect the data it collected, assuring its customers that it is "committed to protecting [members'] privacy."[1] Despite this assurance to its customers, however, SAG Health failed to protect the very customer information it was entrusted, compromising the personal information of an undisclosed number of its members ("**The Data Breach**"), announced by Defendant on December 2, 2024.[2]

3. SAG Health failed to properly secure and safeguard the highly valuable,

1 SAG-AFTRA Health Plan Privacy Policy, SAG-AFTRA Health Plan (2019), https://www.sagaftraplans.org/health/privacy (last accessed December 5, 2024).

2 SAG-AFTRA Health Plan Email Phishing Notice, SAG-AFTRA Health Plan (2024), https://www.sagaftraplans.org/health/emailphishingnotice (last accessed December 5, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

PII and PHI of its members, including members' names, Social Security numbers, and information associated with claims and health insurance information, and other sensitive medical and non-medical data (collectively, "**Private Information**"), failed to comply with industry standards to protect information systems that contain Private Information, and failed to provide timely and adequate notice to Plaintiffs and other members of the Class that their Private Information had been accessed and compromised.

4. As a result of SAG Health's inadequate security and breach of its duties and obligations, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unauthorized criminal third party. Plaintiffs and Class Members have suffered injuries as a direct and proximate result of Defendant's conduct. These injuries include: (i) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their Private Information; (ii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) the continued, long term, and certain increased risk that unauthorized persons will access and abuse Plaintiffs' and Class Members' Private Information; (iv) the continued and certain increased risk that the Private Information that remains in Defendant's possession is subject to further unauthorized disclosure for so long as Defendant fails to undertake proper measures to protect the Private Information; (v) invasion of privacy and increased risk of fraud and identity theft; (vi) theft of their Private Information and the resulting loss of privacy rights in that information; (vii) diminution in value and/or lost value of Private Information, a form of property that Defendant obtained from Plaintiffs and Class Members. This action seeks to remedy these failings and their consequences. Plaintiffs and Class Members have a continuing interest in ensuring that their Private Information is and remains safe, and they should be entitled to injunctive and other equitable relief.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

5. Even the most fundamental Private Information, like names, email addresses, home addresses, or phone numbers, when paired with other uniquely personalized data like health insurance information, Social Security numbers, and health plan identification numbers, become especially valuable to cybercriminals to create seemingly legitimate, personalized phishing scams. This exfiltrated personal data, the full extent of which SAG Health has failed to disclose to the public, allows hackers to gain a clear image of each individual and track their whereabouts, leading hackers to each victim's behavior and background. The combined exfiltrated data effectively provides criminals with a key to their personal lives, making it easy to match additional data, gaining access to their personal accounts and insight on their preferences. Hackers are now able to build a three-dimensional picture, and thereby exploit SAG Health's members.

6. SAG Health disregarded the rights of Plaintiffs and Class Members by, inter alia, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to properly train its staff and employees on proper security measures.

7. In addition, SAG Health failed to properly monitor its computer network and systems that housed the Private Information. Had it properly monitored these electronic and cloud-based systems, it would have discovered the intrusion sooner or prevented it altogether.

8. Defendant has also been unjustly enriched. When members enroll in Defendant's Plan, they are paying for not only the benefits offerings themselves but also for proper data management and security. Defendant should have invested a greater portion of the monies received from Plaintiffs and Class Members in proper data management and security, including proper and safe storage of Plaintiffs' and

Class Members' Private Information. Because Defendant failed to implement data management and security measures sufficient to protect that data and comply with industry standards, the principles of equity and justice demand that Defendant not be permitted to retain the money Plaintiffs and Class Members paid Defendant for protection they did not receive.

9. Plaintiffs bring this lawsuit on behalf of themselves and all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained. To remedy these violations of law, Plaintiffs and Class Members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendant's data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

## PARTIES

### I. PLAINTIFFS

10. **Plaintiff Rouillard.** Plaintiff Matthew Rouillard only allowed Defendant to maintain, store, and use his Private Information because he reasonably expected that Defendant would use basic security measures to protect his Private Information and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access accounts or databases storing his Private Information, exercising appropriate managerial control to require employee training in recognizing and thwarting social engineering attacks, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Rouillard entrusted his Private Information to Defendant, and his Private Information was within the possession and control of Defendant at the time of the Data Breach. Had Plaintiff Rouillard been informed of Defendant's insufficient data security measures to protect his Private Information, he would not have willingly provided his Private Information to Defendant.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

11. Plaintiff Rouillard has been a SAG-AFTRA member since 2012 and has been enrolled in the SAG Health Plan since 2016. Plaintiff Rouillard received a notice of data breach from Defendant on December 2, 2024. Plaintiff Rouillard pays approximately $375 per quarter to receive coverage under the SAG Health Plan.

12. **Plaintiff Munden.** Plaintiff Kristy Munden only allowed Defendant to maintain, store, and use her Private Information because she reasonably expected that Defendant would use basic security measures to protect her Private Information and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access accounts or databases storing her Private Information, exercising appropriate managerial control to require employee training in recognizing and thwarting social engineering attacks, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Munden entrusted her Private Information to Defendant, and her Private Information was within the possession and control of Defendant at the time of the Data Breach. Had Plaintiff Munden been informed of Defendant's insufficient data security measures to protect her Private Information, she would not have willingly provided her Private Information to Defendant.

13. Plaintiff Munden has been a SAG-AFTRA member since 1988, and her most recent enrollment period began in 2022.

14. At the moment Plaintiffs' Private Information was accessed and obtained by a third party without their consent or authorization, Plaintiffs suffered injury from a loss of privacy. Plaintiff Munden pays approximately $375 per quarter to receive coverage under the SAG Health Plan.

15. As a result of the Data Breach, Plaintiffs have been further injured by the damages to and loss in value of their Private Information -a form of intangible property that Plaintiffs entrusted to Defendant. This information has inherent value that Plaintiffs were deprived of when their Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

16. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiffs to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of their Private Information. This highly sensitive information, which includes their ***name, Social Security number, and information associated with claims and health insurance information***, is now in the hands of criminals as a direct and proximate result of Defendant's misconduct.

17. As a result of the actual harm Plaintiffs have suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiffs to spend significant time and energy dealing with issues related to the Data Breach, including self- monitoring their accounts to ensure no fraudulent activity has occurred, investigating fraudulent activity, alerting their banking services about the breach, and changing identifying information and passwords for her accounts. Much of the time and energy that Plaintiffs expended, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

18. The substantial risk of imminent harm and loss of privacy has also caused Plaintiffs to suffer stress, fear, emotional distress, and anxiety.

19. Defendant acknowledged the risk posed to Class Members and their Private Information as a result of the Data Breach, explicitly stating that "We take this matter very seriously," encouraging members to "be on alert for any suspicious activity related to their financial accounts and credit reports" and to "regularly monitor their credit report, statements, and records to ensure that there are no transactions or other activities that were not initiated or authorized by them."[3]

## II. DEFENDANT

20. **SAG Health.** Defendant is a labor-management trust established under

[3] *SAG-AFTRA Health Plan Email Phishing Notice*, supra note 2.

California law, with its principal place of business in the city of Burbank. Defendant conducts business, providing health benefits to eligible participants, across the nation.

## JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section 1332(d) because this is a class action where the aggregate amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367. Furthermore, the affected victims of the data breach – the Class Members – reside nationwide.

22. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District: Defendant's principal place of business is located in this District from where its board of directors and/or officers direct Defendant's activities including to their actions and inactions leading to the data breach at issue; Defendant gains revenue and profits from doing business in this District; Class Members were affected by the breach from SAG Health's actions and inactions directed from this District.

## FACTUAL ALLEGATIONS

23. SAG Health is a provider of health and medical benefits servicing tens of thousands of SAG-AFTRA members and their families primarily in California and New York. Defendant collects and processes the personal data of its members. To avail themselves of benefits coverage, members are forced to entrust Defendant with their Private Information.

24. The information collected and stored by Defendant includes, but is not limited to, ***names, Social Security numbers, and information associated with claims and health insurance information***.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

25. Defendant holds itself as a trustworthy company, which recognizes and values its members' privacy and personal information and has repeatedly assured its members that it "understands that your health information is personal, and we are committed to protecting it."[4] Defendant doubles down on its commitments, warranting that "we pledge that we will take reasonable steps to ensure that your Personal Information . . . will be only used in ways that are in compliance with this Privacy Policy."[5] The "Personal Information" that Defendant pledged to protect includes the Private Information compromised in the Data Breach; specifically, Defendant defines "Personal Information" in the same Privacy Policy as "(1) contact information (e.g. name)… (6) social security number… (8) [members'] health care ID number."[6]

26. Defendant's privacy policy clearly and unequivocally states that any personal information provided to Defendant will be vigorously protected.

27. Plaintiffs and other similarly situated members relied to their detriment on Defendant's uniform representations and omissions regarding data security, including Defendant's failure to alert customers that its security protections were inadequate, and that Defendant would forever store Plaintiffs' and members' Private Information, failing to archive it, protect it, or at the very minimum warn consumers of the anticipated and foreseeable data breach.

28. Had Defendant disclosed to Plaintiffs and its other members that its data systems were not secure and were vulnerable to attack, Plaintiffs would not have enrolled in Defendant's health benefits coverage, paid (or overpaid) premiums to

---

[4] *Notice of Privacy Practices* (2023). SAG-AFTRA Health Plan, from https://www.sagaftraplans.org/sites/default/files/inline-files/Notice%20of%20Privacy%20Practices%2001-2023%20%28from%20SPD%29.pdf (last accessed December 5, 2024).

[5] *SAG-AFTRA Health Plan — Health and Privacy*. (2019). SAG-AFTRA Health Plan, from https://www.sagaftraplans.org/health/privacy (last accessed December 5, 2024).

[6] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

receive health benefits coverage, or utilized its other services. Defendant would have been forced to adopt reasonable data security measures and comply with the law.

29. Plaintiffs and other similarly situated members trusted Defendant with their sensitive and valuable Private Information.

## I. The Data Breach

30. At all material times, SAG Health failed to maintain proper security measures despite its promises of safety and security to consumers.

31. On September 18, 2024, Defendant became aware that an employee's email account had been compromised; specifically, on September 16th and 17th, there was unauthorized access to Defendant's internal systems. Defendant did not notify its customers then, nor made any announcements to alert of this major security issue. By October 3, 2024, Defendant concluded that members' information was likely acquired.[7] Yet again, Defendant chose not to notify the affected customers for the next several months.

32. On around December 2, 2024, Defendant finally began notifying some members of the Data Breach, including Plaintiff Rouillard, when nearly three months had passed since learning of the unauthorized access and two months had passed since Defendant concluded that personal information had likely been acquired.

33. In its statement, Defendant does not disclose how many members' Private Information was breached, leaving consumers to speculate whether it is likely that their PII/PHI has been compromised and without any clear instruction on what they can do to protect themselves now that their Private Information has been exposed. Instead, Defendant downplayed the extent of the Data Breach, and the likely harm affected victims may experience.

## II. Data Breaches and the Market for PII/PHI

34. When a victim's data is compromised in a breach, the victim is exposed

[7] *SAG-AFTRA Health Plan Email Phishing Notice*, *supra* fn 2.

to serious ramifications regardless of the sensitivity of the data—including but not limited to identity theft, fraud, decline in credit, inability to access healthcare, as well as legal consequences.[8]

35. The U.S. Department of Justice's Bureau of Justice Statistics has found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that resolution of those problems could take more than a year.[9]

36. The U.S. Government Accountability Office (GAO) has concluded that it is common for data thieves to hold onto stolen data for extended periods of time before utilizing it for identity theft.[10] In the same report, the GAO noted that while credit monitoring services can assist with detecting fraud, those services do not stop it.[11]

37. When entities entrusted with personal data fail to implement industry best practices, cyberattacks and other data exploitations can go undetected for a long period of time. This worsens the ramifications and can even render the harm irreparable.

38. PII is a valuable commodity for which a black market exists on the dark web, among other places. Personal data can be worth from $1,000-$1,200 on the dark

[8] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_ V2_combinedWEB.pdf (last accessed December 5, 2024).
[9] U.S. Department of Justice, Bureau of Justice Statistics, Victims of Identity Theft, 2014 (Sept. 2015), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last accessed December 5, 2024).
[10] U.S. Government Accountability Office Report to Congressional Requesters, Data Breaches – Range of Consumer Risks Highlights Limitations of Identity Theft Services, https://www.gao.gov/assets/700/697985.pdf (last accessed December 5, 2024).
[11] *Id.*



Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

web[12] [13] and the legitimate data brokerage industry is valued at more than $250 billion.

39. Medical data is even more valuable because unlike other personal information, such as credit card numbers which can be quickly changed, medical data is static. This is why companies possessing medical information, like Defendant, are targeted by cyber-criminals.[14]

40. A 2021 report by Invisibly, a team of application developers focused on reclaiming users' data, found that personal medical information is one of the most valuable pieces of information within the market for data. The report noted that "[i]t's worth acknowledging that because health care records often feature a more complete collection of the PII User's identity, background, and personal identifying information (PII), health care records have proven to be of particular value for data thieves." While a single SSN might go for $0.53, a complete health care record sells for $250 on average.[15]

[12] Ryan Smith, *Revealed-how much is personal data worth on the dark web?*, INSURANCE BUSINESS MAGAZINE, https://www.insurancebusinessmag.com/ca/news/cyber/revealed--how-much-is-personal-data-worth-on-the-dark-web-444455.aspx (last accessed December 5, 2024).

[13] Maria LaMagna, *The sad truth about how much your Google data is worth on the dark web*, MARKETWATCH (last accessed May 21, 2024). 17 Emily Wilson, The Worrying Trend of Children's Data Being Sold on the Dark Web, TNW (February 23, 2019), https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark- web/ (last accessed December 5, 2024).

[14] Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS (September 24, 2014), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (last accessed December 5, 2024).

[15] *How Much is Your Data Worth? The Complete Breakdown for 2024*, INVISIBLY (July 13, 2021) https://www.invisibly.com/learn-blog/how-much-is-data-worth/ (last accessed May 21, 2024).



Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

| Record Type | Average Price |
|---|---|
| Health Care Record | $250.15 |
| Payment Card Details | $5.40 |
| Banking Records | $4.12 |
| Access Credentials | $0.95 |
| Social Security Number | $0.53 |
| Credit Record | $0.31 |
| Basic PII | $0.03 |

41. Medical records are even worth more than an SSN, credit card, and driver's license combined, according to federal officials. They estimate that medical records can go for anywhere between $250 to $1,000.[16]

42. In this black market, criminals seek to sell stolen data to identity thieves who desire the data to extort and harass victims, take over victims' identities in order to open financial accounts, and otherwise engage in illegal financial transactions under the victims' names.

43. PII has a distinct, high value—which is why legitimate companies and criminals seek to obtain and sell it.

[16] Wilkinson, Kate. *RI hospitals fight cyberattacks on 'almost a daily basis',* WPRI (Oct. 10, 2023), https://www.wpri.com/target-12/ri-hospitals-fight-cyberattacks-on-almost-a-daily-basis/ (last accessed December 5, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

44. Medical information in particular is extremely valuable to identity thieves as the medical industry has also experienced disproportionally higher numbers of data theft events than other industries. According to a report by the Health Insurance Portability and Accountability Act Journal, "healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past nine (9) years, with 2018 seeing more data breaches reported than any other year since records first started being published."

45. A study done by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that most victims of medical identity theft were forced to pay out of pocket costs for healthcare they did not receive to restore coverage.[17] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.

46. It should be no surprise that in today's digital economy the "world's most valuable resource is no longer oil, but data."[18] As such, personal information is a valuable property right.[19] Its value is axiomatic, considering the value of "big data" in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that personal information has considerable market value.

47. In a consumer-driven world, the ability to capture and use consumer data to shape products, solutions, and the buying experience is critically important to a

---

[17] See Elinor Mills, Study: *Medical Identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed December 5, 2024).

[18] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.

[19] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[20]

48. Indeed, an entire economy exists related to the value of personal data. In 2022, the big data technology market was valued at roughly $309 billion, and that value is expected to grow to $842 billion by 2023.[21]

49. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[22] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[23] OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military [record] is estimated to cost USD 55."[24]

50. Defendant knew or should have known that Plaintiffs' and Class Members' Private Information is valuable, both to legitimate entities, like Defendant, and to cybercriminals.

---

[20] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

[21] Big Data Technology Market Research Report, Fortune Business Insights (Sept. 2023), https://www.fortunebusinessinsights.com/industry-reports/big-data-technology-market-100144

[22] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

[23] *Id.* at 25.

[24] *Id.*



Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

51. Defendant knew or should have known that Plaintiffs and Class Members would reasonably rely upon and trust Defendant's promises regarding security and safety of their data and systems, and that their valuable Private Information would be protected.

52. By collecting, using, selling, monitoring, and trafficking Plaintiffs' and other members' Private Information, and failing to protect it by maintaining inadequate security systems, failing to properly archive the Private Information, allowing access of third parties, and failing to implement security measures, Defendant caused harm to Plaintiffs and other SAG Health plan members.

## III. The Sensitivity of Members' Private Information Demands Heightened Protection

53. Entities in the healthcare industry are popular targets for cyberattacks and require top-tier security measures to protect PII/PHI, especially given that these databases store sensitive patient records.

54. Ponemon Institute, an expert in the annual state of cybersecurity, indicated in 2020 that organizations storing PHI were top targets for cyber-attacks. In fact, Defendant has been on notice for years that PHI is a prime target for scammers due to the amount and value of confidential patient information maintained. In 2019 alone, numerous entities in the healthcare sector suffered high-profile data breaches, including Quest Diagnostics and LabCorp.

55. In a survey released by Ponemon Institute in January 2023, nearly half of respondents (47%) said their organizations experienced a ransomware attack in the past two years, up from 43% in 2021. And 45% of respondents reported complications from medical procedures due to ransomware attacks, up from 36% in 2021.[25]

[25] Southwick, Ron. *California medical group discloses ransomware attack, more than 3 million affected*, CHIEF HEALTHCARE EXECUTIVE (10 May 2023), https://www.chiefhealthcareexecutive.com/view/california-medical-group-discloses-ransomware-attack-more-than-3-million-affected (last accessed December 5, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

56. Countless victims impacted by the Data Breach now face a constant threat of being repeatedly harmed, including but not limited to living the rest of their lives knowing that criminals can compile, build and amass and build profiles on them for decades – exposing them to a continuing threat of identity theft, disclosure of PII/PHI, threats, extortion, harassment and phishing scams, and the attendant anxiety from not knowing how your information will be used when it comes into nefarious individuals' hands.

57. Data breaches of this caliber can result in the exposure of extremely sensitive information about adults and children's medical histories, medical conditions, psychological assessments, psychiatric evaluations, location of employers, schools, residences, and much more, which poses great dangers on its own – and more importantly poses a great danger not only to SAG members but their minor dependents. The FBI has warned that "widespread collection of student data could have privacy and safety implications if compromised or exploited."[26] Defendant manages health benefit coverage for its members *and their dependents*; its failure to safeguard Private Information puts its members' children at risk.

58. Due to the special risks associated with individuals' data breaches and the increasing frequency with which they are occurring, it is imperative for entities like Defendant to routinely: (a) monitor for system breaches, cyberattacks and other exploitations; (b) update their software, security procedures, and firewalls; and (c) make sure its employees are adequately trained to recognize and thwart social engineering attacks, such as phishing.

## IV. Defendant's Duty to Safeguard Private Information

59. Defendant is responsible for safeguarding the Private Information of tens of thousands of its members, including PII/PHI of those members' families.

[26] Education Technologies: *Data Collection and Unsecured Systems Could Pose Risks to Children*, FBI Alert No. I-091318-PSA (Sept. 13, 2018), https://www.ic3.gov/media/2018/180913.aspx (last accessed December 5, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

60. Defendant collects, receives, and accesses members' extensive individually identifiable information. This Private Information includes names and Social Security numbers, as well as PHI in the form of health insurance information.

61. Defendant was prohibited by the Federal Trade Commission Act (the "**FTC Act**") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "**FTC**") has concluded that an entity's failure to maintain reasonable and appropriate data security for individuals' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

62. The FTC has brought enforcement actions against entities engaged in commerce for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

63. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all decision-making.[27]

64. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for

[27] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed December 5, 2024).
At https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed December 5, 2024).

businesses.[28] The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

65. The FTC further recommends that entities not maintain PII/PHI longer than needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[29]

66. Furthermore, FTC requires that entities like Defendant conduct risk assessments, implement and periodically review access control, encrypt customer information, implement multi-factor authentication for **anyone accessing customer information within their systems**, dispose of customer information securely, maintain a log of authorized users' activity and keep an eye out of unauthorized access, **train employees regarding security awareness**, conduct audits, penetration testing, and system wide scans regularly to test for publicly known security vulnerabilities – all of which if had been properly implemented would have allowed Defendant to prevent this Data Breach.

67. Defendant failed to properly implement basic data security practices, allowing for this social engineering attack to occur, victimizing thousands of people – by failing to adhere to many of the FTC protocols and allowing access to a hacker impersonating an employee. Defendant should have a multifaceted security protocol

[28] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136-protecting-personal-information.pdf (last accessed December 5, 2024).

[29] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed December 5, 2024).



Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

in place, including a program that adequately trains employees on recognizing and thwarting phishing and social engineering attacks, monitoring out-of-network emails, segmenting the network, flagging suspicious domain addresses or content, utilized multifactor authentication before allowing access to highly sensitive information, mandating strict compliance with these protocols; mandating regular archiving of email data/removal of sensitive data from emails to servers; avoiding exchanging any sensitive data for patients/members over the emails, simulating social engineering attempts to ensure compliance, increasing spam filtering via email gateways, implementing strict policies regarding exchange of PII/PHI over emails, implementing and enforcing appropriate credential/key procedures including finger print recognition/physical key authentication; monitoring systems 24/7 for any suspicious activity, encrypting data over the email exchanges. Had Defendant maintained these and other proper protocols and regularly conducted audits to ensure its vulnerabilities and training, it would have prevented this Data Breach.

68. Plaintiffs and Class Members provided their Private Information to SAG Health with the reasonable expectation and mutual understanding that SAG Health would comply with its obligations to keep such information confidential and secure from unauthorized access.

69. SAG Health's failure to provide adequate security measures to safeguard members' Private Information is especially egregious because it operates in a field which has recently been a frequent target of scammers attempting to gain access to confidential PII/PHI, and it had been targeted by an unauthorized individual before[30]. SAG Health should have been on notice that it was an attractive target for cybercriminals in 2019, when it detected unauthorized access on its systems that led to a threat actor using members' financial information to make unauthorized

[30] *FAQs for Data Privacy Event* (2019), AFTRA Retirement Fund, available at https://aftraretirement.org/Home/FAQs/faqs-for-data-privacy-event (Last visited December 5, 2024)

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

purchases.[31]

## V. Impact of the Data Breach on Consumers

70. Plaintiffs and the Class have suffered actual harm as a result of Defendant's conduct. Defendant failed to institute adequate security measures that led to a data breach. This breach allowed hackers to access the Private Information, including ***names, Social Security numbers, and health insurance information,*** of Plaintiffs and the Class. Now that the Private Information has been accessed and absconded with, it is available for criminal elements to sell or trade and will continue to be at risk for the indefinite future. In fact, the U.S. Government Accountability Office found that, "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[32]

71. Plaintiffs and Class Members are now vulnerable to a full gamut of cybercrimes, loss in value of their property, and have been forced to take remedial action, as listed below:

### Digital Phishing Scams

72. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security numbers. Phishing scams are frequently successful, and the FBI reported that people lost approximately $57 million to such scams in 2019 alone.[33]

73. Defendant knew or should have known of the dangers of digital phishing scams. When Personal Information is employed in a social engineering scheme,

---

[31] *Id.*

[32] *See* U.S. GOV'T ACCOUNTABILITY OFF. REPORT TO CONGRESSIONAL REQUESTERS 29 2007. https://www.gao.gov/new.items/d07737.pdf. (Last visited December 19, 2023).

[33] *See How to Recognize and Avoid Phishing Scams*, FTC Consumer Advice, https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (Last visited December 19, 2023).

criminals can gain unfettered access to individuals, or corporate databases, as the Data Breach itself evinces.

74. Defendant's members are now more likely to become victims of digital phishing attacks because of the compromised information.

**SIM-Swap**

75. The data leak can also lead to SIM-swap attacks against the Class. A SIM-swap attack occurs when the scammers trick a telephone carrier to porting the victim's phone number to the scammer's SIM card. By doing so, the attacker is able to bypass two-factor authentication accounts, as are used to access cryptocurrency wallets and other important accounts. The type of personal information that has been leaked poses a profound tangible risk of SIM-swap attacks for the Class.

76. Defendant's members are now more likely to become victims of SIM Swap attacks because of the released personal information.

**Loss of Time**

77. As a result of this breach, Plaintiffs and impacted consumers will suffer unauthorized email solicitations, and experience a significant increase in suspicious phishing scam activity via email, phone calls, text messages, all following the breach. In addition, Plaintiffs, as a result of the breach, have spent significant time and effort researching the breach, monitoring their accounts for fraudulent activity, reviewing unsolicited emails, texts, and answering telephone calls.

**Overpayment**

78. Plaintiffs and the Class paid initiation fees and annual dues to SAG-AFTRA in exchange for services, including health benefits provided by Defendant. Currently, SAG-AFTRA initiation fees are $3,000, and annual dues are $236 plus 1.575% of covered earnings, up to $1,000.[34] Additionally, Plaintiffs and Class

[34] *Membership Costs,* SAG-AFTRA, available at: https://www.sagaftra.org/membership-benefits/membership-costs (Last visited December 4, 2024).



Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

members must pay a premium to enroll in SAG Health Plan. Current rates are due quarterly: $375 for one participant, $531 for one participant and one dependent, and $747 for one participant and two dependents.[35] Plaintiffs and the Class would not have paid the premiums required to receive coverage or would have paid substantially less to receive coverage, if they knew that doing so would result in their Private Information being compromised and exfiltrated. Thus, they significantly overpaid for the services, based on what the services were represented as compared to the services they received.

**Threat of Identity Theft**

79. As a direct and proximate result of Defendant's breach of confidence, and failure to protect Private Information, Plaintiffs and the Class have also been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuse of this Private Information, resulting in ongoing monetary loss and economic harm, loss of value of privacy and confidentiality of the stolen Private Information, illegal sales of the compromised Private Information on the black market, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties; decreased credit scores, lost work time, and other injuries. Defendant, through its misconduct, has enabled numerous bad actors to sell and profit off of Private Information that belongs to Plaintiffs.

**Out of Pocket Costs**

80. Plaintiffs are now forced to research and subsequently acquire credit monitoring and reasonable identity theft defensive services and maintain these services to avoid further impact. Plaintiffs anticipate spending out of pocket expenses to pay for these services.

[35] *Premium Due Dates* (2024), SAG-AFTRA Health Plan, available at: https://www.sagaftraplans.org/health/premiums (Last visited December 5, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

81. Upon information and belief, Defendant also used Plaintiffs' Private Information for profit and continued to use Plaintiffs' Private Information to target Plaintiffs and share their information with various third parties for Defendant's own benefit.

**Diminution in Value of a Valuable Property Right**

82. Because personal data is valuable personal property, market exchanges now exist where internet users like Plaintiffs and Class Members can sell or monetize their own personal data.

83. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to legitimate marketers or app developers.[36] For example, consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year[37].

84. Accordingly, as a result of the Data Breach, Plaintiffs lost the sale value of their Private Information and the opportunity to control how it is used. That a threat actor specifically targeted Defendant demonstrates just how valuable Plaintiffs' Private Information can be to hackers and the significant value of Plaintiffs' Private Information to cybercriminals.

**Summary of Actual Economic and Noneconomic Damages**

85. In sum, Plaintiffs and similarly situated consumers were injured as follows:

i. Theft of their Private Information and the resulting loss of privacy rights in that information;

ii. Improper disclosure of their Private Information;

iii. Loss of value of their Private Information;

[36] *See, e.g.*, *The Personal Data Revolution*, DATACOUP, https://datacoup.com/

[37] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

iv. The amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures;

v. Defendant's retention of profits attributable to Plaintiffs' and other customers' Private Information that Defendant failed to adequately protect;

vi. Economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiffs are now exposed;

vii. Ascertainable out-of-pocket expenses and the value of Plaintiffs' time allocated to fixing or mitigating the effects of this data breach;

viii. Overpayments for Defendant's products and/or services which Plaintiffs paid to enroll in;

ix. Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this data breach.

## VI. Defendant Should Have Invested in Appropriate & Necessary Data Security

86. In the years immediately preceding the Data Breach, Defendant knew or should have known that its computer systems were a target for cybersecurity attacks.

87. The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity and Infrastructure Security Agency, State Attorney General Offices and many other government and law enforcement agencies, and hundreds of private cybersecurity and threat intelligence firms, have issued warnings that put Defendant on notice, long before the Data Breach, that (1) cybercriminals were targeting companies who store personal health information, such as Defendant; (2) cybercriminals were ferociously aggressive in their pursuit of large collections of Private Information like that in possession of Defendant; (3) cybercriminals were selling large volumes of Private

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Information and corporate information on Dark Web portals; and (4) the threats were increasing.

88. Had Defendant been diligent and responsible, it would have known about and acted upon warnings published in 2017 that 93% of data security breaches were avoidable and the key avoidable causes for data security incidents are:

- Lack of a complete risk assessment, including internal, third-party, and cloud-based systems and services;
- Not promptly patching known/public vulnerabilities, and not having a way to process vulnerability reports;
- Misconfigured devices/servers;
- Unencrypted data and/or poor encryption key management and safeguarding;
- Use of end-of-life (and thereby unsupported) devices, operating systems, and applications;
- Employee errors and accidental disclosures — lost data, files, drives, devices, computers, improper disposal;
- Failure to block malicious email; and
- **Users succumbing to business email compromise (BEC) and social exploits.**[38]

89. In light of the information and warnings readily available to Defendant before the Data Breach, Defendant had reason to be on guard and to increase data security to avoid an attack.

90. Further, Defendant suffered a data breach in 2019, yet did not employ sufficient remedial measures to prevent additional breaches in the future.

91. Prior to the Data Breach, Defendant thus knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' Private Information could be accessed, exfiltrated and utilized by nefarious individuals as the result of a cyberattack.

---

[38] Gretel Egan, *OTA Report Indicates 93% of Security Breaches Are Preventable*, PROOFPOINT (Feb. 7, 2018), available at https://www.proofpoint.com/us/security-awareness/post/ota-report-indicates-93-security-breaches-are-preventable (last accessed May 19, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

92. Prior to the Data Breach, Defendant knew or should have known that it should ensure its employees with access to the Private Information are adequately trained in recognizing and thwarting social engineering attacks, such as the phishing attack which led to the Data Breach.

93. Data security experts advise that "the vast majority of data breaches are preventable" if companies follow widely-available advice on data security practices, including "continually audit[ing] and reevaluat[ing]" their data security practices; being aware of and working proactively to counter cybercriminals' evolving techniques and approaches; and training and re-training their employees.[39]

94. Defendant did not follow this advice; nor did it otherwise remedy the inadequacies that it knew led to the first breach of its systems. On its own website, Defendant provides the link to Online Security Tips posted by the U.S. Department of Labor, including the requirement to use strong and unique password, avoid using repat passwords, changing passwords frequently, using Multi-factor authentication, keeping personal contact information current, deleting/closing unused accounts, avoiding Wi-Fi networks, being vigilant of phishing attacks, avoiding clicking links/providing information to unverified entities even if they appear to look like trusted organizations, and other similar tips. Had Defendant enforced strict compliance with these tips, this Data Breach would have been preventable.

## CLASS ALLEGATIONS

95. Plaintiffs bring this action on their own behalf and on behalf of all other persons similarly situated. The Class which Plaintiffs seek to represent comprises:

> "All persons whose Private Information was accessed, compromised, or stolen in the Data Breach

[39] Nate Nead, *How To Prevent A Data Breach In Your Company*, FORBES BUSINESS COUNSEL, FORBES (Jul. 30, 2021) available at https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/30/how-to-prevent-a-data-breach-in-your-company/?sh=3828f7b918da (last accessed December 4, 2024).

announced by Defendant on December 2, 2024" (the "Class").

Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

96. The California Subclass which Plaintiffs seek to represent comprises:

"All persons who currently reside in California and whose Private Information was accessed, compromised, or stolen in the data breach announced by Defendant on December 2, 2024" (the "California Subclass").

Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

97. The Class is comprised of tens of thousands of SAG-AFTRA Health Plan members throughout the United States and the state of California (the "Class Members"). The Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court.

98. There is a well-defined community of interest in the questions of law and fact involved affecting the parties to be represented in that the Class was exposed to the same common and uniform false and misleading advertising and omissions. The questions of law and fact common to the Class predominate over questions which may affect individual Class members. Common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant's conduct is an unlawful business act or practice within the meaning of Business and Professions Code section 17200, *et seq*.;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

b. Whether Defendant's conduct is an unfair business act or practice within the meaning of Business and Professions Code section 17200, *et seq*.;

c. Whether Defendant's conduct is an unlawful business act or practice within the meaning of Business and Professions Code section 17200, *et seq*.

d. Whether Defendant's conduct is in violation of California Civil Code §§ 1798, *et seq*.;

e. Whether Defendant's conduct is in violation of California Civil Code §§ 56, *et seq*.;

f. Whether Defendant's conduct is in violation of California Civil Code Sections 1709, 1710;

g. Whether Defendant's failure to implement effective security measures to protect Plaintiffs' and the Class's Private Information was negligent;

h. Whether Defendant breached express and implied warranties of security to the Class;

i. Whether Defendant represented to Plaintiffs and the Class that it would protect Plaintiffs' and the Class members' Private Information;

j. Whether Defendant owed a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

k. Whether Defendant breached a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

l. Whether Class Members' Private Information was accessed, compromised, or stolen in the Data Breach;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

m. Whether Defendant's conduct caused or resulted in damages to Plaintiffs and the Class;

n. Whether Defendant failed to notify the public of the breach in a timely and adequate manner;

o. Whether Defendant knew or should have known that its systems, including but not limited to training protocols and policies, left it vulnerable to a data breach;

p. Whether Defendant adequately addressed the vulnerabilities that allowed for the Data Breach; and

q. Whether, as a result of Defendant's conduct, Plaintiffs and the Class are entitled to damages and relief.

99. Plaintiffs' claims are typical of the claims of the proposed Class, as Plaintiffs and Class Members were harmed by Defendant's uniform unlawful conduct.

100. Plaintiffs will fairly and adequately represent and protect the interests of the proposed Class. Plaintiffs have retained competent and experienced counsel in class action and other complex litigation.

101. Plaintiffs and the Class have suffered injury as a result of Defendant's false, deceptive, and misleading representations.

102. Plaintiffs would not have given their Private Information to Defendant but for the reasonable belief that Defendant would safeguard their data and Private Information.

103. The Class is identifiable and readily ascertainable. Notice can be provided to such purchasers using techniques and a form of notice similar to those customarily used in class actions, and by internet publication, radio, newspapers, and magazines.

104. A class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of individual litigation

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually.

105. The litigation and resolution of the Class's claims are manageable. Individual litigation of the legal and factual issues raised by Defendant's conduct would increase delay and expense to all parties and the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive supervision by a single court.

106. Defendant has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and/or corresponding declaratory relief appropriate with respect to the Class as a whole. The prosecution of separate actions by individual Class Members would create the risk of inconsistent or varying adjudications with respect to individual member of the Class that would establish incompatible standards of conduct for Defendant.

107. Absent a class action, Defendant will likely retain the benefits of its wrongdoing. Because of the small size of the individual Class Members' claims, few, if any, Class Members could afford to seek legal redress for the wrongs complained of herein. Absent a representative action, Class Members will continue to suffer losses and Defendant (and similarly situated companies) will be allowed to continue these violations of law and to retain the proceeds of its ill-gotten gains.

**COUNT ONE**

**VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW**

**BUSINESS & PROFESSIONS CODE SECTION 17200, *et seq.***

**(ON BEHALF OF THE CALIFORNIA SUBCLASS AND NATIONWIDE CLASS)**

108. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

109. For all Class members outside of the California Subclass, these claims are brought under the relevant consumer protection statute for the state in which they reside. For each state, the relevant statutes are as follows: Alabama—Deceptive Trade Practices Act (Ala. Code § 8-19-1, *et seq.*); Alaska—Unfair Trade Practices and Consumer Protection Act (Alaska Stat. § 45.50.471, *et seq.*); Arizona—Consumer Fraud Act (Ariz. Rev. Stat. Ann. § 44-1521, *et seq.*); Arkansas—Deceptive Trade Practices Act (Ark. Code Ann. § 4-88-101, *et seq.*); Colorado—Consumer Protection Act (Colo. Rev. Stat. § 6-1-101, *et seq.*); Connecticut—Connecticut Unfair Trade Practices Act (Conn. Gen. Stat. § 42-110a, *et seq.*); Delaware—Consumer Fraud Act (Del. Code Ann. tit. 6, § 2511, *et seq.*); District of Columbia—D.C. Code § 28-3901, *et seq.*; Florida—Deceptive and Unfair Trade Practices Act (Fla. Stat. § 501.20, *et seq.*); Georgia—Fair Business Practices Act (Ga. Code Ann. § 10-1-390, *et seq.*); Hawaii—Haw. Rev. Stat. § 480-1, *et seq.*); Idaho—Consumer Protection Act (Idaho Code Ann. § 48-601, *et seq.*); Illinois—Consumer Fraud and Deceptive Business Practices Act (815 Ill. Comp. Stat. 505/1, *et seq.*); Indiana—Deceptive Consumer Sales Act (Ind. Code § 24-5-0.5-1, *et seq.*); Iowa—Iowa Code § 7.14.16, *et seq.*); Kansas—Consumer Protection Act (Kan. Stat. Ann. § 50-623, *et seq.*); Kentucky—Consumer Protection Act (Ky. Rev. Stat. Ann. § 367.110, *et seq.*); Louisiana—Unfair Trade Practices and Consumer Protection Law (La. Rev. Stat. Ann. § 51:1401, *et seq.*); Maine—Unfair Trade Practices Act (Me. Rev. Stat. Ann. tit. 5, § 205A, *et seq.*); Maryland—Maryland Consumer Protection Act (Md. Code Ann., Com. Law § 13-101, *et seq.*); Massachusetts—Regulation of Business Practice and Consumer Protection Act (Mass. Gen. Laws Ann. ch. 93A, §§ 1-11); Minnesota—False Statement in Advertising Act (Minn. Stat. § 8.31, Minn. Stat. § 325F.67), Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68, *et seq.*); Mississippi—Consumer Protection Act (Miss. Code Ann. § 75-24, *et seq.*); Missouri—Merchandising Practices Act (Mo. Rev. Stat. § 407.010, *et seq.*); Montana—Unfair Trade Practices and Consumer Protection Act (Mont. Code. Ann. § 30-14-101, *et seq.*); Nebraska—

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Consumer Protection Act (Neb. Rev. Stat. § 59-1601); Nevada—Trade Regulation and Practices Act (Nev. Rev. Stat. § 598.0903, *et seq.*, Nev Rev. Stat. § 41.600); New Hampshire—Consumer Protection Act (N.H. Rev. Stat. Ann. § 358-A:1, *et seq.*); New Jersey—N.J. Stat. Ann. § 56:8-1, *et seq.*); New Mexico—Unfair Practices Act (N.M. Stat. § 57-12-1, *et seq.*); New York—N.Y. Gen. Bus. Law §§ 349, 350, N.Y. Exec. Law § 63(12); North Carolina—N.C. Gen. Stat. § 75-1.1, *et seq.*); North Dakota—N.D. Cent. Code § 51-15-01, *et seq.*); Ohio—Consumer Sales Practices Act (Ohio Rev. Code Ann. § 1345.01, *et seq.*); Oklahoma—Consumer Protection Act (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon—Unlawful Trade Practices Law (Or. Rev. Stat. § 646.605, *et seq.*); Pennsylvania—Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. Ann. § 201-1, *et seq.*); Rhode Island—Unfair Trade Practice and Consumer Protection Act (R.I. Gen. Laws § 6-13.1-1, *et seq.*); South Carolina—Unfair Trade Practices Act (S.C. Code Ann. § 39-5-10, *et seq.*); South Dakota—Deceptive Trade Practices and Consumer Protection Law (S.D. Codified Laws § 37-24-1, *et seq.*); Tennessee—Consumer Protection Act (Tenn. Code Ann. § 47-18-101, *et seq.*); Texas—Deceptive Trade Practices—Consumer Protection Act (Tex. Bus. & Com. Code Ann. § 17.41, *et seq.*); Utah—Consumer Sales Practices Act (Utah Code Ann. § 13-11-1, *et seq.*); Vermont—Consumer Fraud Act (Vt. Stat. Ann. tit. 9, § 2451, *et seq.*); Virginia—Consumer Protection Act (Va. Code Ann. § 59.1-196, *et seq.*); Washington—Consumer Protection Act (Wash. Rev. Code § 19.86.010, *et seq.*); West Virginia—W. Va. Code § 46A-6-101, *et seq.*); Wisconsin—Wis. Stat. § 100.18, 100.20; Wyoming—Consumer Protection Act (Wyo. Stat. Ann. § 40-12-101, *et seq.*).

**A. "Unfair" Prong**

110. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code Section 17200, et seq., a challenged activity is "unfair" when "any injury it causes outweighs any benefits provide to consumers and the injury is one that the consumers

themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

111. Defendant's conduct as alleged herein does not confer any benefit to consumers. Mishandling this data, by failing to train employees responsible for the safeguarding of this data, shows blatant disregard for members' privacy and security.

112. Defendant's conduct as alleged herein causes injuries to members who do not receive health benefit services consistent with their reasonable expectations; specifically, services that would place their Private Information in the hands of cybercriminals.

113. Defendant's conduct as alleged herein causes injuries to its members, who entrusted Defendant with their Private Information and whose Private Information was leaked as a result of Defendant's unlawful conduct.

114. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in law, including the FTC Act, 15 U.S.C. §45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

115. Members cannot avoid any of the injuries caused by Defendant's conduct as alleged herein.

116. The injuries caused by Defendant's conduct as alleged herein outweigh any benefits.

117. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of California Business and Professions Code Section 17200.

118. Defendant could have furthered its legitimate business interests in ways other than its unfair conduct.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

119. Defendant's conduct threatens members by misleadingly advertising its purported "commitment" to protecting Private Information while exposing members' Private Information to hackers. Defendant's conduct also threatens other entities, large and small, who play by the rules. Defendant's conduct stifles competition, has a negative impact on the marketplace, and reduces consumer choice.

120. All of the conduct alleged herein occurs and continues to occur in Defendant's operations. Defendant's wrongful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

121. Pursuant to Business and Professions Code Sections 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unfair business practices.

122. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs relied on and made their health benefit coverage selection in part based on Defendant's representations regarding its security measures and trusted that Defendant would keep her Private Information safe and secure. Plaintiffs accordingly provided their Private Information to Defendant reasonably believing and expecting that their Private Information would be safe and secure. Plaintiffs paid an unwarranted premium for the coverage and services they received. Specifically, Plaintiffs paid for services advertised as secure when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to the Data Breach.

123. Plaintiffs and the Class would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Plaintiffs and Class Members seek an order mandating that Defendant implement adequate security practices to protect members' Private Information. Additionally, Plaintiffs and Class Members seek an order awarding Plaintiffs and the

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

**B. "Fraudulent" Prong**

124. California Business and Professions Code Section 17200, et seq. considers conduct fraudulent and prohibits said conduct if it is likely to deceive members of the public. *Bank of the West v. Superior Court*, 2 Cal. 4th 1254, 1267 (1992).

125. Defendant's advertising and representations that it adequately protects consumer information is likely to deceive members of the public into believing that Defendant can be entrusted with Private Information, and that Private Information gathered by Defendant is not in danger of being compromised.

126. Defendant's representations about its commitments to data security, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes fraudulent conduct.

127. Defendant knew or should have known of its fraudulent conduct.

128. As alleged in the preceding paragraphs, the material misrepresentations by Defendant detailed above constitute a fraudulent business practice in violation of California Business & Professions Code Section 17200.

129. Defendant could have implemented robust security measures to prevent the Data Breach but failed to do so; specifically, Defendant could have ensured that employees with access to Private Information received adequate training to recognize and thwart social engineering attacks.

130. Defendant's wrongful conduct is part of a pattern or generalized course of conduct.

131. Pursuant to Business & Professions Code Section 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its practice of false and deceptive representations about the strength

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

or adequacy of its security systems. Likewise, Plaintiffs and the Class seek an order requiring Defendant to disclose such misrepresentations.

132. Plaintiffs and the Class have suffered injury in fact and have lost money as a result of Defendant's fraudulent conduct. Plaintiffs paid an unwarranted premium for the services they received. Specifically, Plaintiffs paid for services advertised as secure when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to the Data Breach.

133. **Injunction**. Pursuant to Business and Professions Code Sections 17203, Plaintiffs and the Class seek an order of this Court compelling Defendant to implement adequate safeguards to protect consumer Private Information retained by Defendant. This includes, but is not limited to: improving security systems, deleting data that no longer needs to be retained by Defendant, archiving that data on secure servers, adopting adequate and robust training policies and protocols for all employees entrusted with access to Personal Information and notifying all affected consumers in a timely manner.

### C. "Unlawful" Prong

134. California Business and Professions Code Section 17200, et seq., identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.,* 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

135. Defendant's unlawful conduct, as alleged in the preceding paragraphs, violates California Civil Code Section 1750, *et seq.*

136. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

137. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, California's Confidentiality

of Medical Information Act, Cal. Civ. Code § 56, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, and California common law.

138. Defendant knew or should have known of its unlawful conduct.

139. As alleged in the preceding paragraphs, the misrepresentations by Defendant detailed above constitute an unlawful business practice within the meaning of California Business and Professions Code section 17200.

140. Defendant could have furthered its legitimate business interests in ways other than by its unlawful conduct.

141. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's unlawful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

142. Pursuant to Business and Professions Code Sections 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unlawful business practices.

143. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs paid an unwarranted premium for Defendant's health plan. Plaintiffs would not have used the services, paying or overpaying for the premiums to receive coverage, if they had known that their use would put their Private Information at risk. Plaintiffs and the Class would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiffs and Class Members seek an order mandating that Defendant implement adequate security practices to protect members' Private Information. Additionally, Plaintiffs and the members of the Class seek and request an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

144. No adequate remedy at law. Plaintiffs and the Class are entitled to equitable relief as no adequate remedy at law exists.

a. Defendant has not yet implemented adequate protections to prevent a future data breach, nor has it given an adequate notice to all affected class members, and therefore, the equitable relief requested here would prevent ongoing and future harm;

b. Injunctive relief is also necessary to prevent the members of general public from being mislead by Defendant's misrepresentations regarding privacy and security of information;

c. The equitable relief under the UCL (and also under unjust enrichment discussed below) creates a straightforward cause of action for violations of law (such as statutory or regulatory requirements related to representations and omissions made with respect to Defendant's services). Furthermore, damages for non-UCL claims require additional elements or pre-suit notice letters, which would potentially eliminate possibility of providing damages to the entire class, while restitution would provide certainty and remedy for all affected victims.

d. In addition, discovery—which has not yet been provided and/or completed—may reveal that the claims providing legal remedies are inadequate. At this time, forcing an election of remedies at the initial pleadings stage, in the absence of completed discovery regarding class certification and merits, is premature and likely to lead to subsequent, potentially belated, and hotly contested motions to amend the pleadings to add equitable remedies based on a lengthy

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

historical recount of discovery and analysis of voluminous exhibits, transcripts, discovery responses, document productions, etc., as well as related motions to seal confidential information contained therein.

**COUNT TWO**

**VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CALIFORNIA CIVIL CODE SECTION 56, *et seq.***

**(ON BEHALF OF THE CALIFORNIA SUBCLASS)**

145. Plaintiffs, individually and on behalf of the California Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

146. Defendant is subject to the requirements and mandates of the CMIA because it is a "health care service plan" pursuant to Cal. Civ. Code § 56.10.

147. CMIA section 56.36 allows an individual to bring an action against a "person or entity who has negligently released confidential information or records concerning him or her in violation of this part."

148. As a direct result of its negligent failure to adequately protect the data it collected from the Plaintiffs and Class Members, Defendant allowed for a Data Breach which released the PII/PHI of Plaintiffs and the Class Members to criminals and/or third parties.

149. The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care ... regarding a patient's medical history, mental or physical condition, or treatment."

150. The CMIA defines individually identifiable information as "medical information [that] includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the [customers]' name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

publicly available information, reveals the individual's identity." Cal. Civ. Code § 56.050.

151. Defendant is in possession of affected individuals' medical insurance and claim information, including, but not necessarily limited to, diagnosis and treatment of patients/customers, laboratory test results, prescription data, radiology reports, and health plan member numbers, with which more data can be ascertained. Further, the compromised data was individually identifiable because it was accompanied by elements sufficient to allow identification of Plaintiffs by the third parties to whom the data was disclosed. Class Members' names were included in the compromised data.

152. Defendant came into possession of Plaintiffs' and Class Members' medical information and had a duty pursuant to Section 56.06 and 56.101 of the CMIA to maintain, store and dispose of the Plaintiffs' and Class Members' medical records in a manner that preserved their confidentiality. Sections 56.06 and 56.101 of the CMIA prohibit the negligent creation, maintenance, preservation, store, abandonment, destruction, or disposal of confidential medical information.

153. Defendant further violated the CMIA by failing to use reasonable care, and in fact, negligently maintained Plaintiffs' and Class Members' medical information, allowing and enabling a threat actor to view and access unencrypted PHI for Plaintiffs and the Class. Plaintiffs' PHI has been misused as a result of Defendant's failure to maintain reasonable security measures and care.

154. Since Defendant maintained Plaintiffs' and class members medical information in California, on California-based servers, where it was ultimately disclosed to third parties, CMIA equally applies to the entire affected Class. *See, e.g., Doe v. Meta Platforms, Inc.*, No. 22-cv-03580-WHO, 2023 U.S. Dist. LEXIS 158683, at *16 (N.D. Cal. Sep. 7, 2023) (holding that another statute, CIPA, could apply to non-residents of California, because the conduct at issue occurred in California).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

155. As a direct and proximate result of Defendant's violations of the CMIA, Plaintiffs and class members have been injured and are entitled to compensatory damages, punitive damages, and nominal damages of one-thousand dollars ($1,000) for each of Defendant's violations of the CMIA, as well as attorneys' fees and costs pursuant to Cal. Civ. Code § 56.36.

**COUNT THREE**

**DECEIT BY CONCEALMENT, CALIFORNIA CIVIL CODE SECTIONS 1709, 1710**

**(ON BEHALF OF THE CALIFORNIA SUBCLASS)**

156. Plaintiffs, individually and on behalf of the California Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

157. Defendant knew or should have known that its security systems were inadequate to protect members' Private Information. Specifically, Defendant had an obligation to disclose to its consumers that its security systems were not adequate to safeguard their Private Information. Defendant did not do so. Rather, Defendant deceived Plaintiffs and the California Subclass by concealing the vulnerabilities in its security systems.

158. Even after Defendant discovered the Data Breach had impacted sensitive Private Information, it concealed it, and waited two months before announcing it to the public so consumers could know and take precautions against the Data Breach.

159. California Civil Code §1710 defines deceit as, (a) "[t]he suggestion, as a fact, of that which is not true, by one who does not believe it to be true"; (b) "[t]he assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true;" (c) "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact;" or (d) "[a] promise, made without any intention of performing it." Defendant's conduct as described herein therefore constitutes deceit of Plaintiffs and the California Subclass.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

160. California Civil Code §1709 mandates that in willfully deceiving Plaintiffs and the California Subclass with intent to induce or alter their position to their injury or risk, Defendant is liable for any damages which Plaintiffs and the California Subclass thereby suffer.

161. As described above, Plaintiffs and the California Subclass have suffered significant harm as a direct and proximate result of Defendant's deceit and other unlawful conduct. Had Defendant been truthful about its security vulnerabilities or had promptly and adequately notified affected parties that their information had been compromised, Plaintiffs and the Class would not have suffered some, if not all, of the harms attributable to the Data Breach. Specifically, Plaintiffs and the Class have been subject to numerous attacks, including various phishing scams. Defendant is liable for these damages.

## COUNT FOUR

## NEGLIGENCE

## (ON BEHALF OF THE NATIONWIDE CLASS)

162. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

163. Defendant owed a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information. This duty included but was not limited to: (a) designing, implementing, and testing security systems to ensure that consumers' Private Information was consistently and effectively protected; (b) implementing security systems that are compliant with state and federal mandates; (c) implementing security systems that are compliant with industry practices; and (d) promptly detecting and notifying affected parties of a data breach.

164. Defendant's duties to use reasonable care arose from several sources, including those described below. Defendant had a common law duty to prevent foreseeable harm to others, including Plaintiffs and Class Members, who were the foreseeable and probable victims of any inadequate security practices.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

165. Defendant had a special relationship with Plaintiffs and Class Members, which is recognized by laws and regulations, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to class members from a data breach. Plaintiffs and Class Members were compelled to entrust Defendant with their PII/PHI. At relevant times, Plaintiffs and Class members understood that Defendant would take adequate security precautions to safeguard that information. Only Defendant had the ability to protect Plaintiffs' and Class Members' PII/PHI stored on its servers.

166. Defendant knew or should have known that Plaintiffs' and the Class Members' Private Information is information that is frequently sought after by criminals.

167. Defendant knew or should have known that Plaintiffs and the Class members would suffer harm if their Private Information was leaked.

168. Defendant knew or should have known that its security systems were not adequate to protect Plaintiffs' and the Class Members' Private Information from a data breach.

169. Defendant knew or should have known that adequate and prompt notice of the data breach was required such that Plaintiffs and the Class could have taken more swift and effective action to change or otherwise protect their Private Information. Defendant failed to provide timely notice upon discovery of the data breach. Some Class Members were informed of the data breach on December 2, 2024. Defendant had learned of the data breach more than two months prior, in September 2024, and learned that consumers' PII was compromised over a month prior, in October 2024.

170. Defendant's conduct as described above constituted an unlawful breach of its duty to exercise due care in collecting, storing, and safeguarding Plaintiffs' and the Class Members' Private Information by failing to design, implement, and maintain adequate security measures to protect this information. Moreover, Defendant did not

implement, design, or maintain adequate measures to detect a data breach when it occurred.

171. Defendant's conduct as described above constituted an unlawful breach of its duty to provide adequate and prompt notice of the data breach.

172. Plaintiffs' and the Class Members' Private Information would have remained private and secure had it not been for Defendant's wrongful and negligent breach of its duties. The leak of Plaintiffs' and the Class Members' Private Information, and all subsequent damages, was a direct and proximate result of Defendant's negligence.

173. Defendant's negligence was, at least, a substantial factor in causing Plaintiffs' and the Class's Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing Class Members' other injuries arising out of the Data Breach.

174. The damages suffered by Plaintiffs and the Class was the direct and reasonably foreseeable result of Defendant's negligent breach of its duties to adequately design, implement, and maintain security systems to protect Plaintiffs' and Class Members' Private Information. Defendant knew or should have known that its security for safeguarding Plaintiffs' and Class Members' Private Information was inadequate and vulnerable to a data breach.

175. Defendant's negligence directly caused significant harm to Plaintiffs and the Class.

## COUNT FIVE

## BREACH OF EXPRESS WARRANTY

## (ON BEHALF OF THE NATIONWIDE CLASS)

176. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

177. Defendant made an express warranty to Plaintiffs and Class Members that it is committed to protecting the Private Information entrusted to it. In order to avail

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

themselves of Defendant's health benefit coverage, Plaintiffs and Class Members were required to provide their Private Information which they reasonably believed, based on Defendant's express representations, would be kept private and secure.

178. Defendant's express warranties regarding its security standards made to Plaintiffs and the Class appears throughout its website.[40] The promises of security associated with the offerings and services describes the offerings and services, specifically relates to the enrollment into Defendant's benefit coverage plan, and therefore becomes the basis of the bargain.

179. Plaintiffs and the Class paid for and enrolled in the health benefits plan with the expectation that the information they provided would be kept safe, secure, and private in accordance with the express warranties made by Defendant on its website.

180. Defendant breached the express warranties made to Plaintiffs and Class Members by failing to provide adequate security to safeguard Plaintiffs' and the Class's Private Information. As a result, Plaintiffs and Class Members suffered injury and deserve to be compensated for the damages they suffered.

181. Plaintiffs and Class Members paid money to enroll in the coverage plan. However, Plaintiffs and Class Members did not obtain the full value of the advertised services. If Plaintiffs and other Class Members had known that their Private Information would be exposed, then they would not have enrolled in and availed themselves of benefit plan.

182. Plaintiffs and the Class are therefore entitled to recover all available remedies for said breach of express warranty, as this Court deems proper.

[40] *See supra* notes 1, 4-5.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

## COUNT SIX

## INVASION OF PRIVACY

## (ON BEHALF OF THE NATIONWIDE CLASS)

171. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

172. Plaintiffs and Class Members had a reasonable and legitimate expectation of privacy in their Private Information that Defendant failed to adequately protect against compromise from unauthorized third parties.

173. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

174. Defendant failed to protect, and released to unknown and unauthorized third parties, the Private Information of Plaintiffs and Class Members.

175. By failing to keep Plaintiffs' and Class Members' Private Information safe, knowingly utilizing unsecure systems and practices, Defendant unlawfully invaded Plaintiffs' and Class Members' privacy by, among others, (i) intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to adequately secure their Private Information from disclosure to unauthorized persons and/or third parties; and (iii) enabling the disclosure of Plaintiffs' and Class Members' Private Information without consent.

176. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider its actions highly offensive.

177. Defendant knew, or acted with reckless disregard of the fact that, organizations handling PHI are highly vulnerable to cyberattacks and that employing inadequate security and training practices would render them especially vulnerable to data breaches.

178. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted, thereby causing Plaintiffs and the Class Members' undue harm.

179. Plaintiffs seek injunctive relief on behalf of the Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiffs and Class Members. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the class.

## COUNT SEVEN

## UNJUST ENRICHMENT

## (ON BEHALF OF THE NATIONWIDE CLASS)

180. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

171. Defendant funds its data security measures entirely from their general revenues, including payments made by or on behalf of Plaintiffs and Class Members.

172. A portion of the payments made by or on behalf of Plaintiffs and Class Members was to be used to provide the necessary level of data security.

173. Plaintiffs and the Class conferred a monetary benefit on Defendant by purchasing the health services from Defendant and in doing so provided Defendant with their most sensitive PII and PHI. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were subject to the transaction and have their PII protected with adequate data security measures.

174. Defendant knew that Plaintiffs and the Class conferred a benefit which it accepted, and through which Defendant was unjustly enriched. Defendant profited from these transactions and used Plaintiffs' and Class's PII and PHI for business purposes to increase their revenues.



Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

175. Defendant enriched itself by saving the costs they reasonably should have spent on the necessary data security measures to secure Plaintiffs' and the Class Members' PII and PHI. Instead of providing the necessary level of security that would have prevented the Data Breach, Defendant instead calculated to increase their own profits at the expense of Plaintiffs and the Class, by using ineffective security measures, failing to pay money for the much needed training of their employees, failing to conduct the audits, implementing other security measures discussed above. Plaintiffs and the Class suffered an injury as a direct and proximate resolute of Defendant's decision to prioritize its own profits over the requisite security and training.

176. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and the Class, because it failed to implement appropriate data management and security measures as mandated by common law and statutory duties.

177. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their PII/PHI nor would have used Defendant's services.

178. Plaintiffs and the Class have no adequate remedy at law as discussed above.

179. Defendant should be compelled to disgorge its profits and/or proceeds that it unjustly received as a result of having Plaintiffs' and Class Members' PII/PHI, or alternatively, Defendant should be compelled to refund the amounts that Plaintiffs and the Class overpaid for services.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, pray for judgment and relief on all cause of action as follows:

A. That the Court determines that this Action may be maintained as a Class Action, that Plaintiffs be named as Class Representatives of the

Class, that the undersigned be named as Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order declaring that Defendant's actions, as set forth in this Complaint, violate the laws set forth above;

C. An order:

a. Prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's utter failure to provide notice to all affected consumers);

b. Requiring Defendant to implement adequate security protocols and practices to protect consumers' Private Information consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;

c. Mandating the proper notice be sent to all affected consumers, and posted publicly;

d. Requiring Defendant to protect all data collected through any account creation requirements;

e. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

f. Requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

g. Requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing,

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

h. Requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;

i. Requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;

j. Requiring Defendant to conduct systematic scanning for data breach related issues;

k. Requiring Defendant to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the Private Information data; and

l. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

D. That the Court award Plaintiffs and the Class damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

E. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiffs and the Class are entitled, including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

F. That the Court award Plaintiffs and the Class pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

G. That the Court award Plaintiffs and the Class their reasonable attorneys' fees and costs of suit;

H. That the Court award treble and/or punitive damages insofar as they are allowed by applicable laws; and

I. That the Court award any and all other such relief as the Court may deem just and proper under the circumstances.

**JURY TRIAL DEMANDED**

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs respectfully demand a trial by jury for all claims.

DATED: December 5, 2024.

**CLARKSON LAW FIRM, P.C.**

*/s/ Yana Hart*

Ryan Clarkson, Esq.
Yana Hart, Esq.
Mark Richards, Esq.
Tiara Avaness, Esq.
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Email:rclarkson@clarksonlawfirm.com
Email:yhart@clarksonlawfirm.com
Email:mrichards@clarksonlawfirm.com
Email: tavaness@clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265